NHS

Bolton Clinical Commissioning Group

Acceptable Use Policy (Including IT, Email and Internet)

Policy Number	**IG004**
Target Audience	**CCG/GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**December 2017**
Last Review Date	**December 2017**
Next Review Date	**December 2019**
Policy Author	**IG Team (GMSS)**
Version Number	**V4.0**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1.0	August 2013	Exec Team	Approval
1.1	June 2015	IG Team	Reviewed & progress to IM & T Operations Board for approval.
2.0	June 2015	IM & T Operations Board	Approved
3.0	June 2017	IG Team	Reviewed & progress to IM & T Operations Board for approval.
4.0	**December 2017**	**CCG Chief Officer**	**Approved**

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1. Introduction and Aims

1.1 This policy is to facilitate effective working within NHS Bolton CCG (henceforth referred to as the CCG). The CCG allows all employees' access to appropriate information systems and technology, including the CCG network, and email. However, with this come risks to the CCG. This policy, therefore, sets out the standards applicable for the use of information and information systems within the organisation.

1.2 This policy covers the following areas for acceptable use:

- Responsibilities and use of IT Assets
- Use of Email and Internet
- Network Usage

1.3 Any applications, e.g.: NHS Mail will also be subject to the NHS terms and conditions of use and their acceptable use policy.

1.4 The aims of this document are to:

- ensure users are aware of their responsibilities in the use of the GMSS (Greater Manchester Shared Services) information systems and CCG information;
- ensure legal and statutory requirements are met; and minimise risk of inadvertent, accidental or deliberate unauthorised access or disclosure of information;
- establish a common set of governance and usage criteria for sending, receiving and storing emails that are to be uniformly applied throughout the CCG and its constituent businesses;
- promote awareness of and adherence to the CCG information governance practices;
- provide a foundation for procedures and processes that support the working practices of the organisation.

1.5 This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

1.6 For the purposes of this policy the aforementioned will be referred to as users throughout the remainder of this document

2. Accountability, Responsibilities and Training

2.1 The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

2.2 The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

2.3 Overall responsibility for the Acceptable Use Policy lies with the Senior Information Risk Owner who has delegated responsibility for managing the development and implementation of procedural documents to the IT Service Supplier and line managers.

2.4 The GMSS Information Governance Team will provide IG advice and guidance in line with contractual obligations and support CCG management where applicable.

2.5 Line managers will take responsibility for ensuring that the Acceptable Use Policy is implemented within their group or directorate.

It is the responsibility of each employee to adhere to the policy.

Users will receive instruction and direction regarding the policy from a number of sources:

- policy/strategy and procedure manuals;
- line manager;
- specific training course;
- other communication methods, for example, team meetings; and staff intranet

2.6 Users must be aware that it may be a disciplinary offence to make disparaging or libellous remarks about their employer, patients or other employees even when using their own computer at home on social networking sites.

2.7 The CCG requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by e-mail. Users must not send any messages containing such material. Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal. If any user is subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation they are encouraged to contact their line manager / HR advisor immediately.

2.8 All users are mandated to undertake the “Introduction to Information Governance” module, the GMSS IG Team will direct staff to the current module. Information Governance training is required to be undertaken on an annual basis.

Where relevant, further training and education will be required of staff. Staff will be informed via the Information Governance Training Needs Analysis.

3. Definition of Terms

3.1 Information Asset

Information assets are definable information resources owned or contracted by an organisation that are 'valuable' to the business of the organisation.

3.2 Malware

Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (MALicious softWARE) but as a general term it deals with all forms of viruses, spyware, Trojans and other software designed with malicious intent.

3.3 Spam

Mass unsolicited electronic mail received from an un-requested source which attempts to convince the user to purchase goods or services. SPAM consumes valuable network resources while delivering no business benefit.

3.4 Blogging or Tweeting

This is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video Examples of blogging websites include Twitter.com and Blogging.com.

3.5 Social Media

This is the term commonly used for web-based and other mobile communications technologies that enable messages and opinions to be shared in dialogue with others.

3.6 Social Networking

This is the use of interactive web based sites or social media sites, allowing individuals on-line interactions that mimic some of the interactions between people with similar interests that occur in life. Popular examples include Facebook.com and Linkedin.com

3.7 Social Engineering or Blagging

This is the method whereby an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation's staff or maintenance contractor etc.

3.8 Intellectual Property Breach

Data / information is a valuable commodity, and much like any other market economy, principles of supply and demand drive it. As risks increase and profits decline, cybercriminals are on the rise. Intellectual Property breach can include unauthorised access, copying or disclosure of a research protected by trade mark, copyrighted materials, and other such information.

3.9 Cyber Security

Is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorised access. Becomes more important as more devices are connected to the Internet.

4. Main Principles

4.1 All data and information relating to the CCG residing on the GMSS information systems remains the property of the CCG at all times, unless otherwise stated.

4.2 Users accept that personal use of the GMSS information systems and equipment is not a right and must be exercised with discretion and moderation. Users further accept the CCG will not accept any liability, in part or whole, for any liability for claims arising out of personal use of the GMSS information systems and equipment or CCG information..

4.3 The CCG retains the right to:

- Request the monitoring of the use of its information systems for the purpose of protecting its legitimate concerns;
- prohibit personal use of information systems without warning or consultation whether collectively, where evidence points to a risk to the CCG and / or constituent businesses, or individually where evidence suggests a breach of this or any other CCG or NHS Policy may have occurred.

4.4 Users are not permitted to access, attempt to access, circumvent, attempt or cause to circumvent, established security mechanisms or controls to view, modify, delete or transmit information and/or information systems to which they have not been given explicit access or authorisation.

4.5 Users are not permitted to share their, or others, usernames and passwords to gain access to any CCG or other information system.

4.6 Users are not permitted to access any information to which they have not been given explicit authorised access.

4.7 Users must follow established procedures for password changes and are not permitted to disclose or write down their passwords.

4.8 Users are strictly prohibited from installing software on their CCG or other NHS supplied device.

4.9 It is mandatory for all users to lock their terminals, workstations, laptops, by pressing ctrl/alt/del (or "windows key" and L), iPads and / or Smartphones when not using the device, even for a short period.

4.10 Authorised Staff and IT users will be permitted to use their personal devices to connect to a CCG network, but will not be permitted to connect to the CCG Corporate domain. In doing so, they must abide by all policies, standards, processes and procedures.

4.11 Illegal downloads, copying and/or storage of copyrighted content onto the CCG information systems is strictly prohibited. (Refer to the section on Prohibited Use – Internet for further information).

4.12 All users must follow Health and Safety guidelines when using information systems.

4.13 Users will adhere to Management guidelines; the Records Management Policy and information on encryption when sharing, or sending CCG information internally or externally (Secure Transfer of Information Guidance Policy).

4.14 Users are strictly prohibited from:

- using CCG information systems and information in a manner that will:
  - break the law and / or have legal implications or liability to the CCG and / or constituent businesses;
  - cause damage or disruption to the CCG information systems, including that of its constituent businesses;
  - violate any provision set out in this or any other policy, or contravene the CCG Standards of Business Conduct and waste time, decrease productivity or prevent the user from performing their primary responsibilities for the CCG,
- initiating the forwarding of chain letters, junk e-mail and/or jokes. If a user receives such an email, the use should immediately report it to their line manager or the IT Service Desk.
- promoting any kind of business, or business activity, except that of the CCG.
- accessing / using personal e-mail accounts, such as Yahoo, Google and Hotmail to forward or receive work e-mails.

4.15 Usage of the CCG Internet is primarily for business use. Occasional and reasonable personal use is permitted, e.g. during breaks, provided that such use does not interfere with performance of duties and does not conflict with CCG policies, procedure and contracts of employment.

4.16 Users must at all times comply with the Copyright, Design and Patents Laws, when downloading material from internet sites.

4.17 The CCG prohibits access to websites deemed inappropriate and monitors access and usage. The monitoring information may be used to support disciplinary action.

4.18 Sites deemed inappropriate are those with material that is defamatory, pornographic, sexist, racist, on-line gambling, terrorism and/or such sites whose publication is illegal or risks causing offence.

4.19 Users must not circumvent, cause to circumvent or use tools to circumvent prohibited website controls. If a user inadvertently accesses an inappropriate website, the user must immediately inform their line manager or the IT Service Desk.

4.20 Financial transactions are not permitted on websites requiring software to be downloaded prior to the transaction being executed. The CCG accepts no responsibility for any charges and/or losses incurred in relation to personal purchases or personal transactions using the CCG information systems regardless of cause. Users are prohibited from having personal items delivered to CCG premises.

4.21 The use of the CCG information systems to conduct on-line selling is strictly prohibited.

4.22 Only the CCG approved standard and supported Instant Messaging software may be used for business purposes. Users must not circumvent, cause to circumvent, or use tools to circumvent established security and controls applied to any GMSS Instant Messaging or other communications software.

4.23 Only the CCG approved, standard and supported software for web conferencing and collaborative working must be used. The use of telephony conferencing software such as Skype and/or Web conferencing such as ‘Go To Meetings’ is strictly prohibited.

4.24 Those staff issued with mobile computing devices including, but not limited to, tablet PCs, laptops, netbooks, smart phones etc., must ensure that the equipment is secure at all times.

4.25 Equipment should not be left on desks overnight and must be locked securely away. Such devices should be transported securely, not left in the car overnight, however they may be locked in the boot during the day where there is no suitable alternative.

4,26 Users of mobile computing devices will not allow unauthorised access by third parties including, but not limited to, family and friends.

5. Prohibited Use of the Internet

5.1. Use of the internet for the following is strictly forbidden at any time, and anyone using the Internet inappropriately may be disciplined and/or prosecuted

- Pornography (e.g. accessing child pornography is illegal)
- Illegal or commercial activities (e.g. sites promoting violence, racial discrimination or sexual harassment, sites that are defamatory or that are intended to harass or intimidate other staff or using NHS resources to operate a business from work or advertising)
- Activities for financial gain (e.g. lotteries, gambling)
- Downloading material protected by copyright unless express permission has been given (Copyright Designs and Patents Act 1988)
- Hacking (e.g. breaking into other computer systems using the NHSR network as a conduit)
- Fraud (e.g. providing false details or attempting to gain profit illegally

If users have any questions about what is considered to be appropriate or inappropriate use, they are advised to check with their line manager or the IT Department. Known sites falling within the above categories may be blocked by web security software.

Any user requiring access to a site that has been blocked by the web security software should contact the GMSS IT Service Desk in the first instance on 0161 765 6685.

6. Emails

6.1 It is the responsibility of each user to ensure they manage their e-mail appropriately and routinely delete unwanted e-mails or routinely archive e-mails. Users will not be able to send e-mails once their quota has been reached.

6.2 The CCG reserves the right to monitor e-mail usages and content.

6.3 All e-mails are potentially disclosable to the public under the Freedom of Information Act (FOIA).

6.4 Users must not send personal identifiable data, patient data, sensitive, or confidential information to an insecure e-mail address, for example Yahoo, or auto forwarding of emails from an NHS mail address to a non NHS mail address. Secure e-mail addresses are nhs.net and a number of secure Government networks as listed below. Users should consult their line manager or the IT Service Desk if in doubt.

For clarity: person identifiable, sensitive or confidential information must not be sent unprotected to external non-nhs.net e-mail addresses. For example x.y@CCGA.nhs.uk to x.y@ACUTE.nhs.uk
Non-NHS domains that are secure for the transmission of sensitive data are those with the following suffixes:

- .x.gsi.gov.uk
- .gsi.gov.uk
- .gse.gov.uk
- .gsx.gov.uk
- .police.uk
- .pnn.police.uk
- .cjsm.net
- .scn.gov.uk
- .gcsx.gov.uk>

6.5 Users must not send e-mails to large number of users unless the recipients have been suitably “Blind Copied” (bcc). This practice will ensure e-mail addresses are not visible to all recipients, which may compromise the confidentiality of one or more recipients.

6.6 Users must use care and discretion when drafting emails taking care of the confidential nature of the communication.

6.7 All e-mails must contain an e-mail signature that conforms to CCG Corporate Guidelines.

7. Monitoring and Review

7.1 This policy will be monitored through staff awareness and supporting evidence to the NHS IG Toolkit

7.2 Users of the Internet must be aware that each site they visit is recorded and logs of sites may be examined to ensure inappropriate usage is dealt with. A full security audit trail may be maintained of records/sites accessed.

7.3 This Policy will be reviewed on an annual basis, and in accordance with the following on an as and when required basis:

- legislative changes;
- good practice guidance;

- case law;
- significant incidents reported;
- new vulnerabilities; and
- changes to organisational infrastructure

7.4 Equality Analysis

The CCG aims to design and implement services, policies and measures that are fair and equitable. As part of its development, this policy and its impact on staff, patients and the public have been reviewed in line with the CCG legal equality duties. The purpose of the assessment is to improve service delivery by minimising and if possible removing any disproportionate adverse impact on employees, patients and the public on the grounds of race, socially excluded groups, gender, disability, age, sexual orientation or religion/belief.

The Equality Analysis has been completed and has identified impact or potential impact as "no impact"

8. Legislation and related documents

- The Data Protection Act 1998 (including the relevant specific codes of practice e.g. Employment Practices & CCTV)
- Freedom of Information Act 2000 (FOIA)
- The Computer Misuse Act 1990
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Regulation of Investigatory Powers Act 2000

9. Other relevant Procedural Documents

- Corporate Information Security Policy
- Confidentiality and Data Protection Policy
- Secure Transfer of Information Procedure

This list is not exhaustive